# SPT (SIP Penetration Tests) User's Manual

Version: 1.0
Date: October 4th 2011
Copyright ©2011 CESNET, z.s.p.o.
Contact: fillip@cesnet.cz

# Contents

1. SPT Overview ..... 3
1.1. Modules ..... 3
1.1.1. Scanning and Monitoring Module ..... 3
1.1.2. Denial of Service Module ..... 3
1.1.3. Registration Manipulation Module ..... 4
1.1.4. SPIT Module ..... 4
2. Getting Started ..... 4
2.1. Autentication via eduID.cz ..... 4
2.2. Autentication via direct accounts ..... 5
3. Configuration and Module Settings ..... 6
3.1. New Test ..... 6
3.1.1. Scanning and Monitoring Module ..... 6
3.1.2. Denial of Service Module ..... 8
3.1.3. Registration Manipulation Module ..... 10
3.1.4. Spam over Internet Telephony Module ..... 11
3.2. Results ..... 12
3.3. Documentation ..... 13
3.4. Logout ..... 13

# 1. SPT Overview

The SPT system serves as a simulator of penetration testing for SIP VoIP communication servers in order to check this important element for currently most commonly occurring attacks and threats. Based on these penetrations the analysis is done and the tester will receive feedback in the form of e-mail notification with test results. Currently the system consists of 4 test modules, but this number will gradually increase of further simulations. The system was designed as a LAMP (Linux, Apache, MySQL, PHP) server and its complete administration including the installation is carried out via a web interface. System is focused mainly on realization of the tests from the public network, so there is no need to be in the same LAN as the tested SIP devices.

## 1.1. Modules

As mentioned above, the SPT system now includes four test modules, which currently represent the most common threats in IP telephony. Individual modules are described below in detail.

### 1.1.1. Scanning and Monitoring Module

In order to be able to carry out an efficient and precise attack on a SIP server, the potential attacker needs to find out the most information about a particular component. This is why we first developed a Scanning and Monitoring ("S&M") module for the SPT system, which is used to test the security of the central against attacks aimed at obtaining information by means of common and available tools.

### 1.1.2. Denial of Service Module

One of the most frequently occurring attacks is DoS (Denial of Service). In reality, it consists of several attacks with the same characteristic feature – to lock up or restrict the availability of the attacked service so that it does not function properly. Several types of DoSs can be used to achieve this; our system tests the SIP server using the most frequently used one, Flood DoS. The principle of the attack is to send a large volume of adjusted or otherwise deformed packets to the target component so that it is unable to provide its core services. As a result of the attack, CPU load increases and most of the available bandwidth is consumed, resulting in the SIP server being unable to service regular calls, or only a minimum amount of them.

### 1.1.3. Registration Manipulation Module

Once the potential perpetrator obtains information about existing accounts, he can manipulate these accounts quite easily. The SPT system we developed can also test SIP servers' security, i.e. measures against manipulating the registration. To carry out this test, the system substitutes the legitimate account registration with a fake, non-existing one. This type of attack can easily be expanded to a so called MITM, Man-in-the-Middle. In this attack, a non-existent user is substituted by a valid SIP registration and all incoming signaling and media to the legitimate registration will be re-directed to the newly created registration.

### 1.1.4. SPIT Module

Today, one of the most popular attacks on the Internet is spam. It is estimated that spams account for 80 - 90% of total attacks on the Internet. Security experts predict that Spam over Internet Telephony (SPIT) will be a major threat in the future. The level of annoyance is even greater than with classical spam. This module tests the SIP server vulnerability against this attack, which goal is to sent automatic calls with prerecorded messages.

# 2. Getting Started

## 2.1. Autentication via eduID.cz

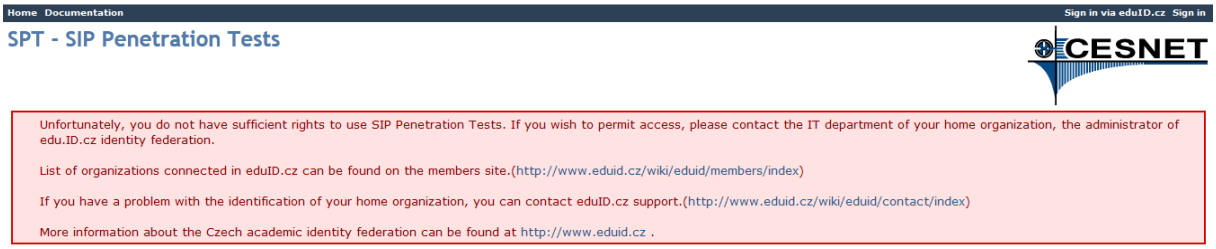
The SPT system is available at **https://pentest.cesnet.cz** as a web application. You must first log in and authenticate against eduID.cz federation, which provides its members a framework for mutual use of the identities of users to control access to network services, while respecting privacy. The list of members is given below:

- Akademie múzických umění
- CESNET, z. s. p. o.
- České vysoké učení technické v Praze
- Českoslovanská Akademie Obchodní Dr. Edvarda Beneše – under connection into federation
- Knihovna Akademie věd České republiky
- Masarykova univerzita
- Mendelova univerzita v Brně
- Moravská zemská knihovna v Brně
- Národní knihovna České republiky
- Národní technická knihovna – under connection into federation
- Jihočeská univerzita v Českých Budějovicích
- Ostravská univerzita v Ostravě
- Slezská univerzita v Opavě

- Uměleckoprůmyslové museum v Praze – under connection into federation
- Univerzita Jana Evangelisty Purkyně v Ústí nad Labem
- Univerzita Hradec Králové – under connection into federation
- Univerzita Karlova v Praze
- Univerzita Palackého v Olomouci
- Univerzita Pardubice
- Ústav pro českou literaturu Akademie věd České republiky – under connection into federation
- Technická univerzita v Liberci
- Vysoká škola báňská - Technická univerzita Ostrava
- Vysoké učení technické v Brně
- Západočeská Univerzita v Plzni

If you are a member of one of the above organizations and if you are interested in using this service, it is necessary that your local eduID.cz administrator has to allow access to the system. More information about the Czech academic identity federation can be found at **http://www.eduid.cz** .

Once you have access through eduID, on the SPT main page, click on the link: *Sign in via eduID.cz* on the upper right corner, select your organization and sign up with your login and password. If the login was successful, you will be redirected to the site of the system itself, otherwise if you have not allowed access through eduID, you will receive the following page:


Home Documentation
Sign in via eduID.cz Sign in
SPT - SIP Penetration Tests
CESNET
Unfortunately, you do not have sufficient rights to use SIP Penetration Tests. If you wish to permit access, please contact the IT department of your home organization, the administrator of edu.ID.cz identity federation.
List of organizations connected in eduID.cz can be found on the members site.(http://www.eduid.cz/wiki/eduid/members/index)
If you have a problem with the identification of your home organization, you can contact eduID.cz support.(http://www.eduid.cz/wiki/eduid/contact/index)
More information about the Czech academic identity federation can be found at http://www.eduid.cz .

## 2.2. Autentication via direct accounts

If your organization is not a member of eduID.cz federation, or you are from abroad, you are even to able to login into SPT system using the direct test accounts. The administrator creates accounts in SPT system (mailto: filip@cesnet.cz) only on the basis of personal consultation. To login using direct accounts, please use link in the upper right corner: *Sign in.*

# 3. Configuration and Module Settings

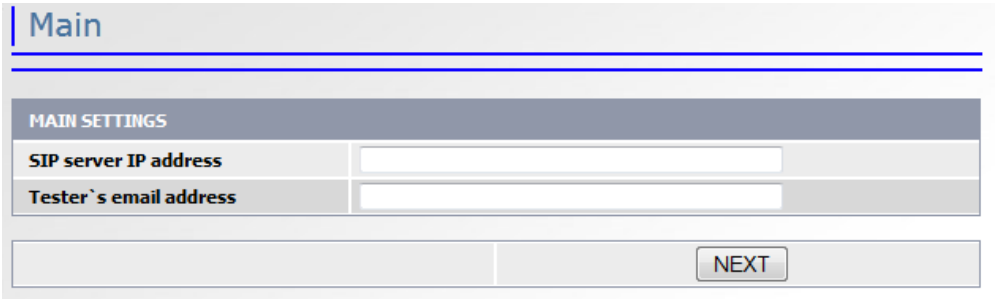
After login you should see a main menu of SPT system. Here you can start a new testing (*New Test*), view the tests results carried out previously bound to the registered person (*Results*), check the user's manual (*Documentation*) or you can logout (*Logout)* from the system.

## 3.1. New Test

The new test is composed of five individual tabs in which the tester fills the appropriate information about the SIP server and parameters for test modules.

The first tab named *Main* contains two forms:

- *SIP server IP address* (required) - tester enters IP address or domain name of SIP server to be tested.
- *Tester's email address* (required) - e-mail address to which the notification with tests results will be sent.




Then click on *NEXT* button for next step.

### 3.1.1. Scanning and Monitoring Module

The second tab called *Scanning and Monitoring (S & M)* is the first of the test tabs. It consists of two tests - *Port Scanning* and *Scanning Extensions*.

- *Port Scanning* (if enabled) – It serves to test open ports through which an attacker could carry out any threats. Both TCP and UDP ports are tested. Tester can either choose a selection of default ports which were selected with a focus on IP telephony or define his/her own range as follows:

  20-2000 – ports from 20 to 2000 will be tested.

  -2000 – ports from 1 to 2000 will be tested.

20- - ports from 20 to 65535 will be tested.

Subsequent e-mail notification will include an overview of test ports and their status. (Please note that testing all of 65535 UDP ports can take up to 18 hours, so use the port range wisely.)

- *Extensions Scanning* (if enabled) - This test can detect the extensions on the target SIP server and possibly a passwords for these accounts using a brute force methods. For testing purposes, tester can choose a default range of extensions (100-999) or manually select his/her own range (1000-9999). The last option for extensions scanning is to insert a text file (.txt) with account names lined up each one on the row. This file may contain alphanumeric names. In addition, the tester can choose SIP method to be used for sending requests to the SIP server. Methods which can be used: REGISTER, INVITE and OPTIONS.

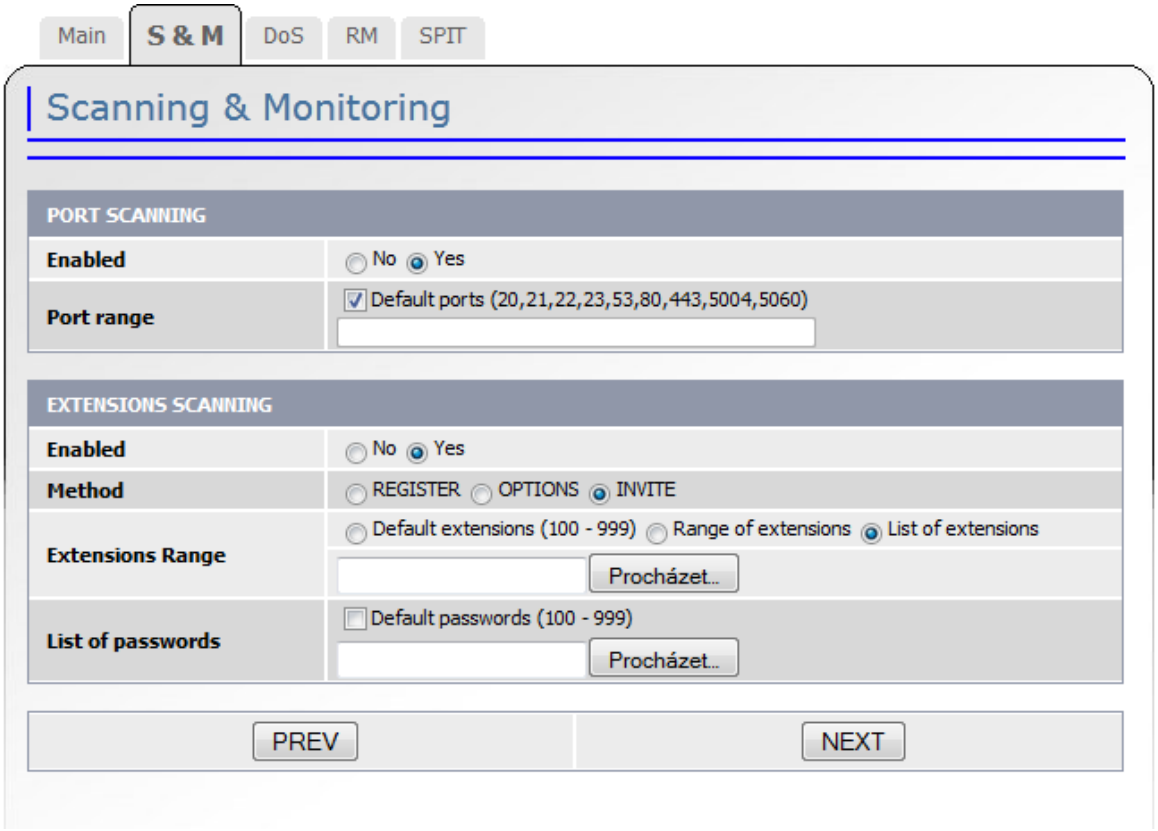
  Another possibility of *Extensions Scanning* is the choice of testing passwords for the founded valid extensions. In this case, the system applies a selected list of passwords on all valid extensions founded on the SIP server in the previous step. This list can be presented by default option (100-999) or by embedded text file (.txt) containing passwords lines up each one on the row.

Then click on *NEXT* button for next step.

Subsequent e-mail notification will include a list of valid extensions founded with state of their required authentication:

- noauth – without authentication (password)
- reqauth - with authentication (password)
- weird - cannot recognize

and the list of extensions founded with valid password.




### 3.1.2. Denial of Service Module

The third tab called *Denial of Service (DoS)* is the second of the test tabs. It consists of two tests – *UDP Flood Test* and *INVITE Flood Test.*

- *UDP Flood Test* (if enabled) - This type of test is intended to send a large number of UDP packets to the target SIP server to attempt to overwhelm a network interface or run out of computing capacity. Tester enters only the number of packets that want to send. Packets are automatically delivered to port 5060, which is the default port for the SIP protocol.

Verification that the test was successful is done by comparing the ping response times before, during and after the Denial of Service test. If the average response time during or after the test is inherently different from the time before the test, the test is considered successful. Subsequent e-mail notification should include one of the following messages:

- *DoS UDP test was successful* – Test was successful.
- *DoS UDP test is not working. Device is not respond to Ping.* – Test could not be processed because the target SIP server is not responding to ping.
- *DoS UDP test was not successful. The SIP proxy response is ok.* – The ping responses during and after the test were within the permissible limit. Test wasn´t successful.

- *DoS UDP test is not enabled.* – The UDP DoS test was not enabled.

- *INVITE Flood Test* (if enabled) - This type of test is intended to send a large number of INVITE packets to the target SIP server to attempt to overwhelm a network interface or run out of computing capacity. Tester enters the valid SIP extension or leave checked the option *Random Valid Extension*, the SPT system automatically selects one of the valid extensions founded in the previous test - *Extensions Scanning*. Then he/she enters the number of packets that want to send. Packets are automatically delivered to port 5060, which is the default port for the SIP protocol. This DoS test (or attack) is much more insidious for SIP servers, because server must respond on INVITE messages and thus far more computing capacity is lost.

Then click on *NEXT* button for next step.

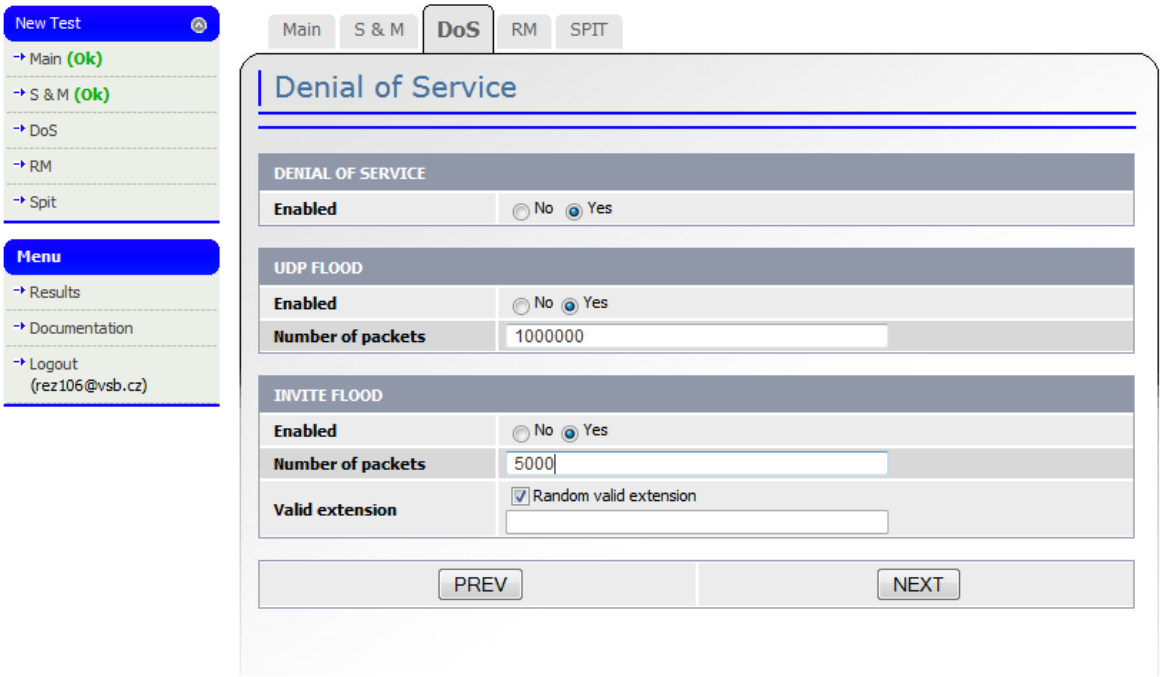
Like UDP DoS, verification that the test was successful is done by comparing the ping response times before, during and after the Denial of Service test. If the average response time during or after the test is inherently different from the time before the test, the test is considered successful. Subsequent e-mail notification should include one of the following messages:

- *DoS INVITE test was successful* – Test was successful.

- *DoS INVITE test is not working. Device is not respond to Ping.* – Test could not be processed because the target SIP server is not responding to ping.

- *DoS INVITE test was not successful. The SIP proxy response is ok.* – The ping responses during and after the test were within the permissible limit. Test wasn´t successful.

- *DoS INVITE test is not enabled.* – The INVITE DoS test was not enabled.




### 3.1.3. Registration Manipulation Module

The fourth tab called *Registration Manipulation (RM)* is the third of the test tabs. It consists of one test – *Registration Manipulation.*

- *Registration Manipulation* - The aim of this test is to check the security of the SIP server on extension registration theft. SPT system will replace an existing account with other non-existent. This effectively prevents incoming calls to be placed on the target account until the re-registration. To realize the test, the valid extension with password is needed. Tester can either manually enter this parameters or can let the SPT system choose one from the founded with the previous *Extensions Scanning* test. He/She can also test all of the valid extensions founded. The system also checks whether the selected account is registered with a SIP client, which is also a necessary condition for a successful test.

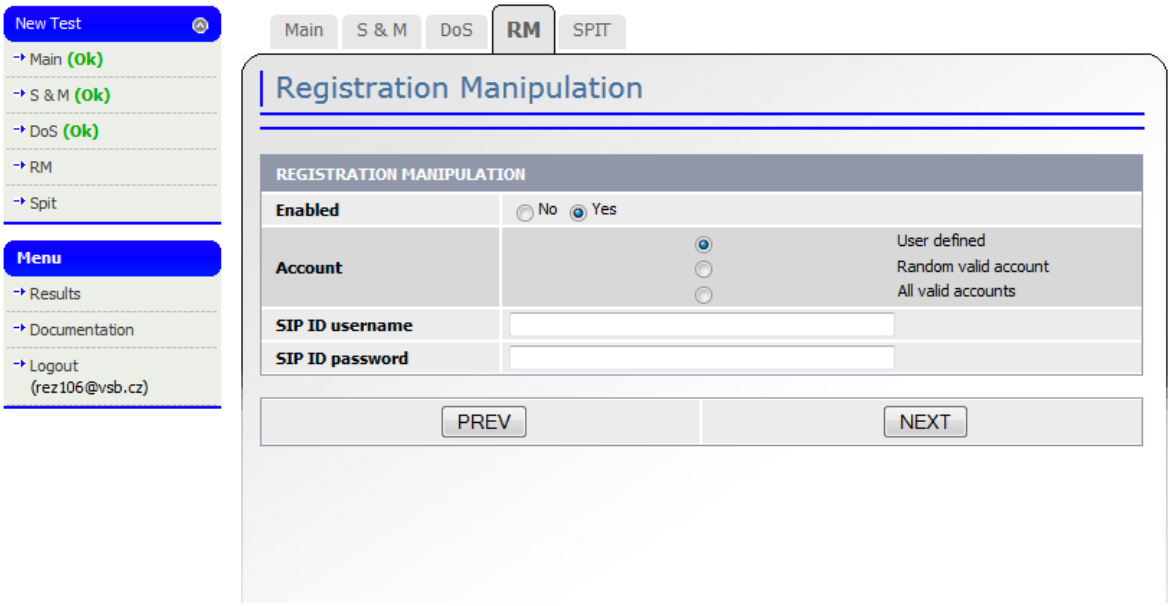
Then click on *NEXT* button for next step.

Subsequent e-mail notification will include a tab with the list of tested accounts, if they were registered and if the test was successful. Example is shown below:

| Tested extensions | Registred | RM Attack successful |
|---|---|---|
| 1000 | yes | yes |
| 1001 | no | no |
| 1002 | yes | yes |

If no valid extensions with passwords are founded in previous *Extensions Scanning* test the following message is sent:

- *The valid account was not found - RM test was not performed.*




### 3.1.4. Spam over Internet Telephony Module

The last tab called *Spam over Internet Telephony (SPIT)* is the fourth of the test tabs. It consists of one test – *Spam over Internet Telephony- SPIT.*

- *SPIT* - In the form, the tester defines the value of a valid SIP account – the called party to which the SPIT call will be directed and then the value and password to a valid SIP account – the caller through which the call will be initiated. Where the tester fails to define these values, the system automatically assigns an account and an appropriate password from the list created while scanning and monitoring the target SIP server. If the test was successful, a SIP call is initiated from the caller's account, and the end device with the registered account of the called party starts ringing. Once the call is answered, a pre-recorded message is played and the call terminated. SPT system repeats the call five times in a row.

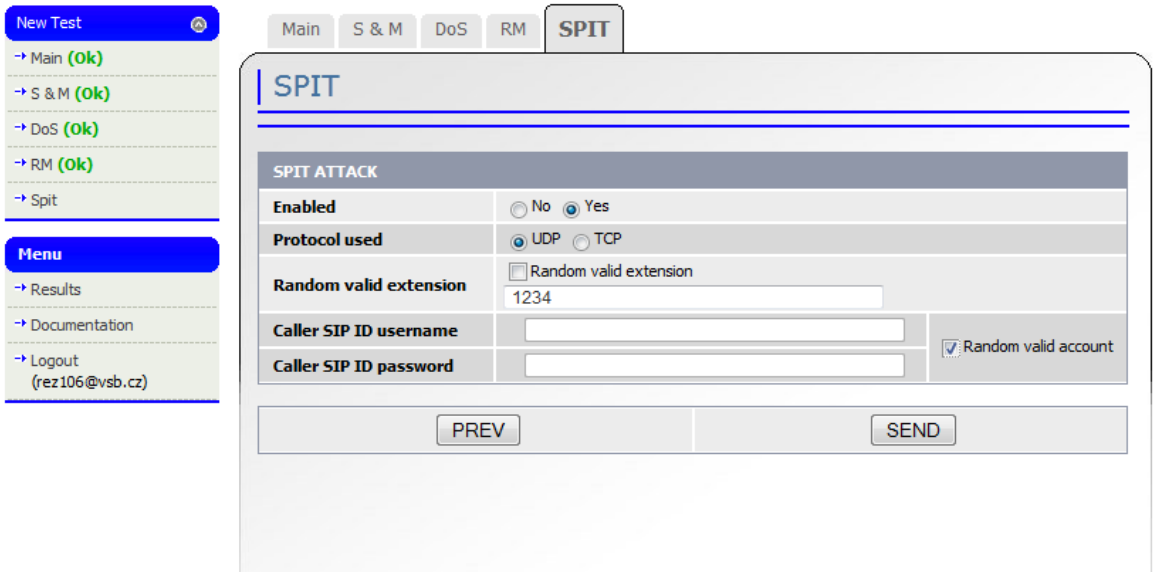
Then click on *SEND* button to start the TEST.

The final report on penetration tests which the tester receives via e-mail, will, besides information on all previous tests, also contain an analysis and success rate of the SPIT module's test. Example is shown below:

```
Results of SPIT test
 ================================================================
  Number of successful calls:        4     (Successful SPIT attacks)
  Number of rejected calls:          0
  Number of timeouted calls:         1
                                   ---------
  Total number of calls:             5
```

If some error appears the corresponding message is sent:

- *SPT system did not find a valid account with a valid password - can not initiate a test.*
- *SPT system did not find a valid extension - cannot initiate a test.*
- *The account match was found - SPIT test was not performed.*



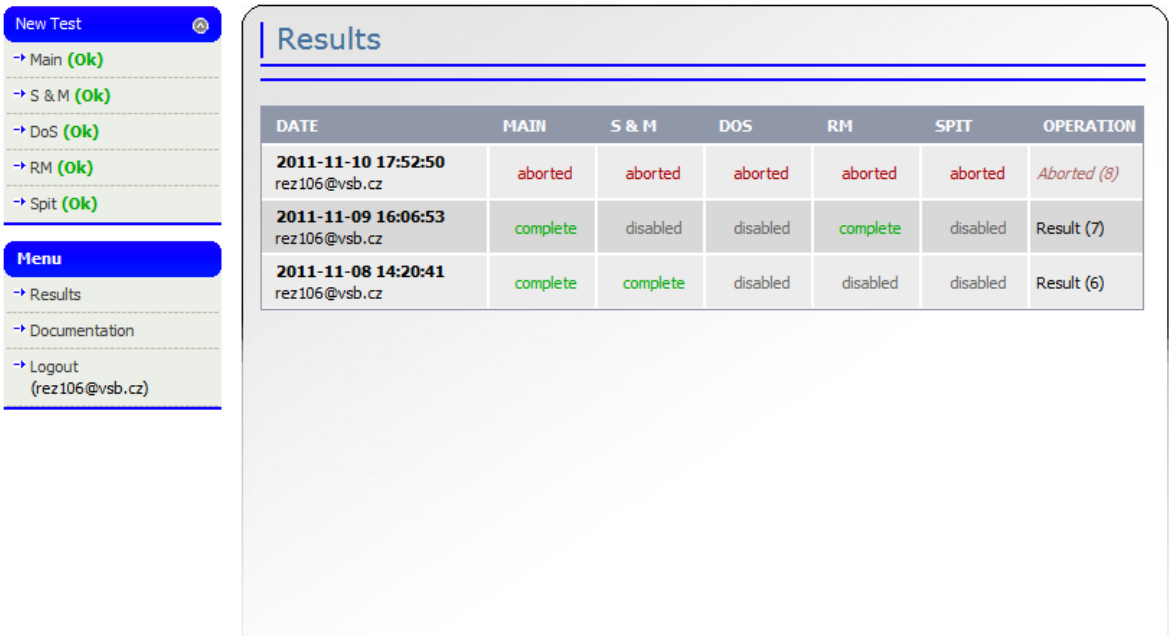

## 3.2. Results

After startup of the New test the tester is redirected to a results page where he/she can watch the actual testing and a list with all tests started before. Once all test modules are finished, email notification with results is sent, or results can be downloaded directly from the Results page (*Result*). Testing can also be canceled by clicking on *Abort*.

Below are described all the states, which may appears during testing:

- ***waiting*** *– test is waiting for run*
- ***working*** *– test runs*

- ***completed*** *– test is done*
- ***disabled*** *– test isn't enabled*
- ***aborted*** *- test was aborted*




## 3.3. Documentation

It refers to the documentation.

## 3.4. Logout

Used to logout from the system.